Statement of

Christopher J. McMahon, RADM, USMS

Departmental Office of Intelligence, Security, and Emergency Response

United States Department of Transportation

Before the

Subcommittee on National Security, Emerging Threats and International Relations

Committee on Government Reform

United States House of Representatives

March 2, 2005

Good afternoon, Mr. Chairman and Members of the Subcommittee, I am Rear Admiral Christopher J. McMahon, United States Maritime Service,[1] United States Department of Transportation (DOT). Recently, I returned from serving in Baghdad, where I was appointed by Secretary Mineta as Transportation Counselor and Senior Iraqi Reconstruction Management Office (IRMO) the Transportation Consultant at the American Embassy. In these positions, I was the principal representative responsible for overseeing transportation infrastructure reconstruction. Currently, I serve in DOT's Office of Intelligence, Security, and Emergency Response. In this capacity, I advise the Secretary on intelligence issues and work closely with the security community, including the Department of Homeland Security (DHS), and other Federal agencies involved with homeland security. I am honored to be here to discuss with you how the Department of Transportation is balancing the need for the secrecy necessary to ensure homeland security with the public's right to know how its Government is carrying out its duties.

At DOT, we adhere to the requirements of the Freedom of Information Act (FOIA) in making determinations about what information sought by the public may be disseminated, and what may be lawfully withheld. FOIA is a law with which we are all familiar – and yet we rely heavily on a large body of common law and commentary to interpret and explain it. We use FOIA not only to determine our responses to public information requests, but also to advise our employees on how they should treat the information that they handle. In the context of protecting information vital to homeland security, we are learning that our principle tool is the authority given to us – and given to DHS – to designate information as "Sensitive Security Information (SSI)." At DOT, we use the designation only to refer to information that Congress has mandated that we protect. We also have an administrative safeguarding designation for sensitive information that is not necessarily related to security that we label as, "For Official Use Only (FOUO)," which I will discuss later in my testimony.

[1] The United States Maritime Service is a voluntary organization established by an Act of Congress for the purpose of training United States civilians to serve on merchant vessels of the United States. Many members of the USMS serve at the United States Merchant Marine Academy, Kings Point, NY (my own normal duty station) and the five State maritime academies.

For many years, DOT's Federal Aviation Administration (FAA) had statutory authority to prevent disclosure of information related to aviation security, termed "Sensitive Security Information (SSI)." In a leading case on SSI, *Public Citizen v. Federal Aviation Administration,* 988 F.2d 186 (D.C. Cir. 1993), the court set forth three aspects of it:

- SSI may be withheld from public disclosure under FOIA.
- The information may be withheld from the public rulemaking record in an informal rulemaking.
- The information may be withheld from discovery in civil litigation.

In response to the attacks upon the United States on September 11, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA) that created within DOT the new Transportation Security Administration (TSA). Under section 114(d) of ATSA, TSA, originally part of DOT, has "responsibility for security in all modes of transportation, including . . . security responsibilities over other modes of transportation that are exercised by DOT." (This authority transferred with TSA when TSA became part of the Department of Homeland Security.) ATSA also transferred from FAA to TSA the authority to designate information as SSI and expanded the scope of that authority to all modes of transportation. When Congress created DHS in the Homeland Security Act of 2002, it not only transferred TSA from DOT to DHS, but also transferred TSA's SSI authority, and gave similar authority to DOT.

Multiple sections of the U.S. Code require that the agency administering SSI authority promulgate regulations specifying the types of information qualifying for SSI treatment. FAA's regulations appeared at 14 CFR Part 191; TSA's appear at 49 CFR Part 1520, and DOT's at 49 CFR Part 15, both entitled "Protection of Sensitive Security Information."

I wish to emphasize that SSI is not a national security classification; hence, individuals need not have formal national security clearances to access SSI. What they must have is a clear "need to know," and they must provide assurances that they understand and will comply with regulations related to the possession and permissible use of SSI. In this way, we can share with other Federal agencies, State, local, and tribal governments, academia, industry, and other persons with a "need to know" information vital to homeland security without fear that we must release that same information to unvetted requestors.

When Secretary Mineta confronted the question of how SSI authority was to be handled within DOT, he took five affirmative steps:

1. He delegated the authority to designate information as SSI to the heads of all of DOT's constituent agencies as to their own modes of transportation, but subject to guidance and direction from the Director of Intelligence, Security, and Emergency Response and the Department's General Counsel (who is the Departmental officer in charge of FOIA). Before the Secretary did this, there was uncertainty about who in DOT could make an SSI determination, with the possibility that virtually anyone would be able to invoke SSI in the Secretary's name.

The delegation provides clarity, structure, and accountability to the process, along with a mechanism to ensure consistency and actual security need.

2. The Secretary specifically directed that the Department not use this authority to evade its responsibilities under FOIA, saying that,

> [t]he authority to determine that information is SSI brings with it the responsibility not only to identify and protect qualifying information, but also not to reduce more than is truly needed the public's right to know how this part of its Government is carrying out its duties. Finding the right balance between protecting what needs to be protected and revealing what should be revealed is important. I expect all of us to give it the attention it deserves.

3. He further directed that we report to him regularly and review any case in which his authority is used to make a decision either to designate information as SSI or not to do so.

4. He is asking DOT's Inspector General to review DOT's implementation of its SSI authority after one year to ensure that the SSI designation process is not being used to improperly exempt information from public disclosure.

5. Finally, he directed that we coordinate with DHS on how our two departments will use their parallel SSI authorities.

My staff is learning day in and day out how truly challenging that charge from the Secretary – to find the right balance between protecting what needs to be protected and revealing what should be revealed -- can be. However, as we use this authority to protect the American people, I have emphasized to the heads of our operating administrations that they keep in mind that our actions must always conform to the law and, with the Secretary's admonition, that we not use this authority to restrict unreasonably the public's right to know how we are carrying out our duties.

As I mentioned, I want to discuss an administrative designation for sensitive information that we use at DOT—For Official Use Only (FOUO). FOUO identifies for our employees information that is sensitive and, therefore, before it is given to anyone outside the Federal Government, they are required to consult with FOIA staff. If the information does not qualify for withholding under FOIA, it must be released.[2]

As I stated earlier, this is not an easy area to understand and apply, particularly to the land modes of transportation, for which security concerns are relatively untested.

---

[2] The full warning that is to be used on such information is: "For Official Use Only. Public release to be determined under 5 USC 552." As provided in the relevant DOT directive (DOT Manual 1640.D, Classified Information Management Manual; Chapter 5, For Official Use Only Information (FOUO), 1997):

"For Official Use Only (FOUO) is not a classified information level. Information requiring FOUO marking is discussed in this document only to ensure knowledge of the requirements for unclassified marked documents. The marking FOUO shall be used only on unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), Section 552, Title 5, U.S. Code."

One final issue deserves attention. Questions have been raised over whether the Department of Transportation used its authority to classify information in the interest of national security to withhold from Congress and the public portions of a staff monograph of the 9.11 Commission. The answer is no, we did not. Let me explain.

In the Summer of 2004, the Department of Justice asked DOT and other agencies to review a draft of a 9.11 Commission staff monograph solely from the perspective of national security classification. The Federal Aviation Administration (FAA) made recommendations on classification of information relating to civil aviation security. (Since primary responsibility for civil aviation security had, by that time, been transferred to DHS, FAA recommended to Justice that DHS be consulted on FAA's recommendations.) FAA submitted its recommendations to Justice in mid-September 2004, within the period set by Justice. FAA had no further involvement with the issue of classifying any portion of a 9.11 Commission staff monograph.

In preparation for today's hearing, DOT's Office of Security reviewed how many original classification decisions DOT has made since 2001. This was not hard to do, since the authority to make original classification decisions is very tightly controlled at DOT; only seven people in all of DOT have original classification authority: The Secretary; Deputy Secretary; Assistant Secretary for Administration and the Assistant Secretary's Director of Security; the Departmental Director of Intelligence, Security, and Emergency Response; and the FAA Administrator and the Maritime Administrator. None of these can make an original classification higher than SECRET.

This was also not hard to do since a central accounting is kept at DOT of any decision originally to classify information. According to that accounting, in FY2001, FAA made one SECRET classification and the United States Coast Guard, now part of DHS, made one. In FY2002, FAA made six SECRET classifications and the Coast Guard made one. In FY 2003 DOT made no original security classifications. In FY2004, we also made no original security classifications.

Mr. Chairman, this concludes my prepared remarks. I would be pleased to respond to your questions.